Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

МЕТОДЫ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОДУКТОВ И СИСТЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В.К. ФИСЕНКО, Д.С. КИМ, М.П. ТУР

Объединенный институт проблем информатики НАН Беларуси

Нормативно-методическая база

Создание нормативно-методической базы (НМБ) в области управления, анализа и оценки риска информационной безопасности (ИБ) началось с авторитетных британских стандартов BS 7799-1:2005 (Практические правила управления информационной безопасностью), BS 7799-2:2005 (Требования к системам управления информационной безопасностью), BS 7799–3:2005 Руководство по управлению рисками информационной безопасности), а затем СТБ ISO/IEC 27001-2016 (Требования по оценке и обработке рисков)**,** СТБ ISO/IEC 27002-2012 (Оценка рисков безопасности) и СТБ ISO/IEC 27005-2012 (Информационные технологии. Методы обеспечения безопасности. Менеджмент рисков информационной безопасности).

Анализ приведенных выше стандартов показал, что существующая НМБ в области управления, оценки и обработки рисков вполне пригодна для проведения результативных практических исследований и разработок.

Анализ методов оценки рисков как основы систематического исследования защищаемой системы.

Выделяют следующие методы анализа рисков, характеризующиеся, в основном, различной глубиной проведения анализа исходных данных:

1. Базовый (основной) метод, суть которого состоит в использовании некоторого унифицированного набора требований к безопасности для всех систем ИТ одновременно.

2. Экспертный метод, который включает в себя проведение неформального, прагматического анализа риска и обычно не требует много ресурсов и времени. Метод не является систематическим или структурированным, а основан на знаниях и опыте некоторого эксперта.

3. Детальный анализ рисков. Данный метод предполагает систематический анализ исходных данных для всех систем ИТ конкретной организации с целью оценки рисков нарушения свойств безопасности ИТ и обоснованного выбора средств защиты, соответствующих заданным требованиям.

4. Комбинированный метод анализа рисков. Он представляется собой сочетание нескольких рассмотренных выше методов.

В ГОСТ Р ИСО/МЭК 31010-2011 дано описание полного комплекта методов оценки риска (всего 31 метод, в том числе 12 базовых методов).

Далее остановимся на практически применяемых базовых и детальных методах оценки рисках.

Подход по отбору базовых методов оценки риска.

Средства защиты, определяемые посредством базовых методов, как правило, реализуются с помощью штатных средств защиты информации, предоставляемых общесистемным программным обеспечением, а также соответствующими продуктами, предоставляемыми специализированными организациями и специфицируемыми в специальных каталогах. Преимущество данного подхода состоит в минимальных затратах стоимостных и временных ресурсов на проектирование средств системы ИБ.

Недостаток данных методов состоит в следующем: если уровень требований к средствам защиты информации для отдельных систем ИТ достаточно высок, то для одних систем он может оказаться чрезмерно завышенным, а для других – слишком низким, в том числе для систем, подверженных наибольшему риску. Соответственно, если все системы ИТ организации имеют только минимальные требования по безопасности, то тогда стратегия анализа рисков, построенная на этих методах, может обладать достаточной функциональностью и быть наиболее экономичной, иначе применение этого метода вряд ли обеспечит удовлетворительные проектные решения по созданию средств ИБ. Следует отметить, что для многих организаций, имеющих невысокие требования к безопасности ИТ, применение базовой стратегии будет наиболее приемлемым решением.

Подход по отбору детальных методов оценки риска.

Детальные методы предполагают систематический анализ исходных данных для всех систем ИТ с целью оценки рисков нарушения свойств безопасности ИТ и обоснованного выбора средств защиты, соответствующих заданным требованиям. Преимущество данных методов состоит в том, что они позволяют на основе системного подхода (всестороннего анализа исходных данных и требований) дифференцированно для каждой из систем осуществить выбор требуемых средств СУБ ИТ.

Кроме этого, полученные с помощью данных методов результаты существенно облегчают сопровождение и модернизацию СУБ ИТ. Недостатком же этих подходов является их ресурсоемкость и, как следствие, высокая цена реализации на практике. Они требуют максимальных затрат времени и усилий.

Стратегия применения базового метода оценки риска.

Требования к защите на основе базового метода могут быть определены посредством использования каталогов средств безопасности, в которых предлагаются некоторые наборы средств для защиты ИТ от наиболее общих угроз. Поэтому все, что требуется для применения базового метода, - это найти в таком каталоге тип системы ИТ, соответствующий рассматриваемой системе, и сравнить состав перечисленных в каталоге средств защиты с уже имеющимися. Недостающие средства защиты, т.е. средства, которые реально не установлены в данной СУБ ИТ, должны быть приобретены или реализованы и введены в состав средств создаваемой или модернизируемой СУБ ИТ.

Стратегия применения метода детальной оценки риска

Детальный подход использует процедуры или шаги, входящие в состав логической схемы метода анализа рисков. Полный список этих шагов и составляют стратегию детального подхода.

Перечень действий этих шагов приведен ниже:

определение состава защищаемых ресурсов;

оценка ценности достояний (ресурсов) и определение взаимосвязи между ними;

определение уже установленных средств защиты;

оценка уязвимостей и соответствующих угроз;

определение меры рисков;

формирование списка целей ИБ;

учет существующих ограничений;

выбор средств защиты; оценка допустимости остаточного риска;

спецификация политики и плана безопасности систем ИТ.

Стратегия применения методов обработки рисков

Ниже приводится вариант стратегии применения методов обработки рисков.

Входные данные. Перечень рисков с назначенными приоритетами. Для определения приоритетов при обработке рисков должны быть разработаны критерии для

оценки рисков с учетом: стратегической ценности обработки информации; критичности затронутых информационных активов; законодательно-нормативных требований и договорных обязательств; оперативного значения и значения свойств доступности, конфиденциальности и целостности информации; ожидания и реакции причастных сторон, а также негативных последствий для нематериальных активов и репутации.

Действие. Должны быть выбраны меры и средства контроля и управления для снижения, сохранения, предотвращения или переноса рисков, а также определен план обработки рисков.

Руководство по реализации. Для обработки риска имеется четыре варианта: снижение риска, сохранение риска, предотвращение риска, и перенос риска.

Варианты обработки риска должны выбираться исходя из результатов оценки риска, предполагаемой стоимости реализации этих вариантов и их ожидаемой эффективности.

Заключение

Анализ действующей нормативно-методической базы, методов оценки и обработки рисков информационной безопасности информационных систем подтвердил наличие в Республики Беларусь достаточно документов и материалов для их практического применения в организациях для подготовки и представления документов по сертификации организации в области риска.

Список литературы

1. Астахов А.М. Искусство управления информационными рисками. М.: ДМК Пресс, 2010. - 312 с., ил.

2. Суханов А. Анализ рисков в управлении информационной безопасностью. Операции с документом. НИП «Информзащита». №11 (120), ноябрь 2008.

3. Сухомлин В.А., Майданский И.С. Методика и средства автоматизации проектирования политики безопасности Информационных Технологий. Московский Государственный Университет им. Ломоносова. "Ломоносовские чтения-98" Секция Вычислительной Математики и Кибернетики. М. 1998.

4. СТБ 34.101.70-2016 Информационные технологии. Методы и средства безопасности. Методика оценки рисков информационной безопасности в информационных системах.

ПОЛУАВТОМАТИЧЕСКИЙ СБОР ЖУРНАЛОВ СРЕДСТВ ДОВЕРЕННОЙ ЗАГРУЗКИ

Д. А. ЭПИКТЕТОВ, А.А. АЛТУХОВ

Московский физико-технический институт (государственный университет)
Закрытое акционерное общество «ОКБ САПР»

Неотъемлемой составляющей работы современных информационных систем является аудит, то есть процесс записи информации о происходящих событиях в какое-либо хранилище (журнал). В современных ОС для этого имеются встроенные средства (например, демон *rsyslogd* в семействе *GNU/Linux* и "Журнал событий" в *Windows*). Они позволяют сохранять информацию о происходящих событиях от различных источников в одном месте, предоставляют приложениям программный интерфейс(API) для записи и чтения журнала, а также предоставляют доступ к журналу пользователю. Используя